Segurança, privacidade e anonimato – guia intermediário

By **Gabriel Camargo** 20/10/2022

Créditos da imagem: Giz Modo

Continuando com a série, passamos ao nível intermediário. Seguindo as orientações presentes nesse nível, o usuário será capaz de completamente mitigar o rastreio de empresas anunciantes e Big Techs em notebooks e desktops, bem como limitar substancialmente o rastreamento de smartphones. O nível de segurança atingido será substancial, juntamente ao anonimato parcial. Para mitigar a maioria das ameaças de privacidade comuns, esse nível será suficiente.

- Compartimentalização de navegação
- Sobre o modo anônimo
- Reservas de valor e transações
- Dicas adicionais
- Apêndice A (alternativas recomendadas)
- Apêndice B (modificação do arquivo de hosts)
- Apêndice C (hardening de sistemas Linux)
- Apêndice D (hardening do Firefox)
- Apêndice E (limpeza com ADB)

Compartimentalização de navegação

A estratégia aqui apresentada completamente mitigará a capacidade de rastreamento do usuário por empresas anunciantes e Big Techs. Para funcionar, é indispensável o uso de uma VPN.

Navegadores como o Google Chrome apresentem bons níveis de segurança, contudo, os produtos da Google são tidos como inimigos da sua privacidade e do seu anonimato. Como essa empresa, e outra gigantes da tecnologia, obtém substancial parcela de seu lucro por meio da venda ou compartilhamento de informações dos usuários, aqueles que desejarem maior privacidade devem procurar alternativas a esses produtos.

O navegador Mozilla Firefox, tido como uma alternativa de privacidade frente ao Chrome, apresenta problemas graves quanto utilizado sem devida configuração. Detalhes de como configurar o Firefox para um elevado grau de privacidade podem ser encontrados no apêndice D.

Navegadores como o Falkon e o Iridium apresentam significativas melhoras no quesito privacidade, sendo projetos de código aberto e configurados previamente com maior nível de privacidade em mente. Contudo, por serem navegadores pouco utilizados, se destacam com suas impressões digitais, bem como não apresentam bom fluxo de atualização. Seu uso não é desaconselhado, mas nota-se a existência de opções superiores.

Cada navegador possui uma impressão digital única. Paradoxalmente, quanto mais você tenta bloquear cookies, rastreadores, scripts, anúncios, etc., mais única a sua impressão digital se torna. Bloquear rastreadores é importante para reduzir as informações disponíveis aos adversários. No entanto, aqui desejamos mitigar a

correlação de sessões para a derivação de uma identidade entre navegadores e dispositivos.

Para elevado grau de segurança e privacidade, é necessário a aplicação de uma estratégia abrangente. Mas ao mesmo tempo é necessário que também seja profunda, empregando compartimentalização e diferentes camadas de ação.

Iniciaremos com os navegadores. A solução para o problema aqui apresentado está em seu isolamento. Compartimentalizando o seu uso, os dados de um não poderão ser correlacionados aos do outro.

Deve-se utilizar múltiplos navegadores para esse propósito. No mínimo, três. As possibilidades são significativas. Por exemplo, devidamente protegido por uma VPN sempre ativa, os navegadores poderão ser: Brave (modificado), Firefox (modificado), LibreWolf e Tor Browser.

Para todas as contas referentes ao Google, quando logado, a utilização de seus serviços apenas poderá ocorrer no Brave. No Firefox, nunca o usuário entrará em sua conta Google, mas poderá acessar serviços, como o Youtube. Contas em redes sociais e de compras online apenas ocorrerão nesse navegador. No LibreWolf, serão realizadas navegações em sites de notícias e pesquisas diversas.

No Tor serão realizadas atividades que necessitam de maior grau de anonimato. Dentre elas, pesquisa por temas sensíveis ou o download de guias e manuais com conteúdo que possam chamar atenção de governos autoritários. Você também pode separar um navegador para acessar as contas que não apresentam seu nome verdadeiro.

Essa é apenas uma possibilidade. Os navegadores e usos podem ser alterados, mas o fundamental é a limitação de uso dada a cada um deles. Essas barreiras não podem ser quebradas.

O bloqueio de JavaScript inviabiliza muitos dos ataques contra a navegação do usuário, sendo de segurança, privacidade ou anonimato, mas, mesmo com seu total bloqueio, uma identidade permanente pode ser estabelecida para aquele navegador em específico, utilizando, por exemplo, à linguagem CSS; por isso, para a completa mitigação de correlação, as atividades devem ser compartimentalizadas.

Pode-se, também, empregar níveis progressivos de privacidade nos navegadores utilizados. Por exemplo, Brave < Firefox < LibreWolf < Tor. O aumento de segurança, privacidade e anonimato traz diminuição da usabilidade, comodidade e praticidade, logo, pode-se, tendo em vista os usos dados a cada um deles, elevar progressivamente seus níveis de acordo com a necessidade.

No Brave, assim como em todos os outros navegadores, analise as configurações, principalmente as relativas à segurança e privacidade. Geralmente, para acessar as configurações, deve-se clicar nos riscos ou pontos no canto superior direito e procurar por “configurações” ou similar.

Como o Tor Browser tenta garantir anonimato por meio da generalização da identidade virtual, evite modificá-lo além das opções apresentadas aqui. Recomenda-se que, quando iniciar o Tor Browser, clique no ícone do escudo, no canto superior direito. Clique em “configurações avançadas de segurança”. Altere o nível de segurança de acordo com as suas demandas pessoais. Caso queira maior nível de anonimato, dificultando o descobrimento do uso do Tor pelo seu provedor de internet, utilize o Tor com a opção de pontes (bridges).

Você poderá combinar uma VPN com o Tor. Para isso, basta iniciar a VPN antes de iniciar o navegador. No entanto, recomenda-se que isso apenas seja feito com VPNs confiáveis e adquiridas de forma anônima, como com Monero.

Como extensões devem ser reduzidas ao mínimo, para a proteção da navegação, são recomendadas apenas duas, não necessitando serem utilizadas em simultâneo. Para a melhor proteção atual contra rastreadores e anúncios na web, recomenda-se o uBlock Origin.

Após realizar a instalação, vá nas configurações e analise os filtros habilitados e os que deseja habilitar. Para habilitar a filtragem dinâmica, marque a opção de usuário avançado, presente na parte final da primeira aba do menu.

Clicando agora no símbolo da extensão, você notará que novas colunas apareceram. Essas colunas são clicáveis. As regras dinamicamente alteradas sobrescrevem as estáticas, derivadas das listas. A coluna do meio representa as regras globais e, a da direita, as regras locais. As entradas em vermelho indicam bloqueio. As verdes indicam conexão. As amarelas indicam que houve bloqueio parcial, os símbolos de “+” e “-” indicando que algumas foram bloqueadas, mas outras foram permitidas. A quantidade desses símbolos indica a intensidade de conexões referentes ao domínio listado na esquerda.

Pode-se alterar as regras de conexão clicando nas colunas, tornando-as vermelhas. Caso queira bloquear um determinado domínio globalmente de forma dinâmica, basta tornar a célula da coluna central vermelha. Para bloquear apenas localmente, torne vermelha a célula da direita. As células locais ficam automaticamente vermelhas quando as globais são bloqueadas, vermelho mais fraco, indicando que as regras foram herdadas. Pode-se, contudo, alterar localmente o bloqueio do domínio no site específico sendo visitado. As regras locais sobrescrevem as globais.

O NoScript bloqueia a execução de scripts em páginas web, bem como limita suas ações para os habilitados. É possível bloquear para sempre ou apenas temporariamente um domínio. Bloquear scripts é uma das maneiras mais rápidas e eficazes de obter elevado nível de proteção e privacidade digital, dificultando a execução de códigos maliciosos presentes nas páginas visitadas, bem como mitigando variados tipos de rastreamento das ações executadas em uma página pelo usuário.

Sobre o modo anônimo

Um mito comum sobre os navegadores trata da navegação anônima. O motivo da confusão inicia com o próprio nome. Na verdade, navegar em modo anônimo não torna sua navegação anônima. O modo anônimo de navegadores como o Chrome e o Firefox geralmente realiza as seguintes modificações: ao ser fechado, o navegador não armazena o histórico de navegação, cache, cookies e outros dados da sessão. Algumas informações permanecem, no entanto, como os sites favoritados. O modo anônimo também impede que sites acessem seu histórico de navegação.

Em outras palavras, o seu endereço IP continua sendo publicamente conhecido, as características do navegador e do dispositivo continuam inalteradas; não modificando informações que possibilitam o rastreio digital, os cookies ainda apresentam potencial de te rastrear entre os sites, os rastreadores presentes durante a navegação permanecem inalterados, seu provedor de internet e o administrador da rede ainda são capazes de monitorar sua navegação, etc.

A maior proteção de privacidade oferecida torna-se, então, voltada para as pessoas que utilizam computadores públicos ou compartilhados. Além do não armazenamento de certos dados na máquina do próprio usuário, sub uma perspectiva abrangente de segurança e privacidade, pouco é verdadeiramente alterado.

Reservas de valor e transações

É recomendado possuir reservas de valor na forma física. Trocas efetuadas em meios físicos deixam menos rastros. Não apenas moeda estatal, mas outros meios físicos de troca de valor pouco regulados, como a prata. Diversifique as possibilidades.

Moedas criptográficas são importantes ferramentas, quando bem utilizadas, para aumentar a liberdade e autonomia do indivíduo. A maioria das criptomoedas, no entanto, não foi desenvolvida com privacidade (muitas nem mesmo com segurança) em mente.

O Bitcoin é uma excelente maneira de transferir até mesmo grandes somas de forma

rápida, segura e não burocrática. O Bitcoin, contudo, não foi pensado para ser um meio de troca privado e/ou anônimo. Adversários estatais facilmente podem identificar os envolvidos em uma transação e verificar quanto dinheiro cada um possui. Existem métodos de tornar o Bitcoin uma moeda mais privada e até anônima, mas são soluções que exigem certo nível técnico e a identidade será eventualmente vazada, seja por descuido momentâneo do usuário ou correlação com outras informações no mundo virtual ou físico.

Com o Bitcoin, perder a privacidade e o anonimato obtidos é muito mais fácil do que ganhar. Com Monero, o oposto ocorre. Essas e outras complicações tecnológicas atuais impedem que o Bitcoin seja verdadeiramente uma moeda capaz de desafiar os poderes estabelecidos.

(A opinião do autor não necessariamente reflete a opinião de toda a equipe do Gazeta Libertária).

Uma melhor alternativa é a Monero (XMR). Ao contrário da maior parte das criptos, sua blockchain não pode ser utilizada para rastrear seus usuários, pois utiliza tecnologias que impedem a análise do histórico de transações ou de um endereço de carteira. Endereços aleatórios são gerados a cada transação, impossibilitando o rastreio ao longo do tempo dos fundos movimentados por alguém. Múltiplos usuários assinam digitalmente uma transação e os montantes não são publicamente revelados. Outra moeda de privacidade é a Zcash. Porém, suas medidas de privacidade são opcionais, enquanto que, com a Monero, são o padrão.

Para a compra, evite utilizar corretoras centralizadas, dando preferência para as descentralizadas ou em P2P. Exemplos são a Bisq e LocalMonero. Para o armazenamento, a carteira recomendada é a Monero GUI. Para grandes quantidades, utilize hardware wallets, como a Trezor.

Dicas adicionais

• Quando não estiver utilizando o Bluetooth, desligue-o. Para fins de ganho monetário, empresas estão começando a utilizar esse sinal para rastrear os movimentos dos consumidores nos estabelecimentos, para entender seus hábitos e oferecer descontos em produtos específicos, baseados nas preferências. Esse sinal de rádio também está sendo utilizado para monitorar os contatos e pessoas próximas ao usuário, então, caso não necessite desses serviços, desligue-o.

• De tempos em tempos, faça seu dispositivo esquecer todas as redes sem fio com as quais ele se conectou um dia. Essas informações podem vazar pelo simples fato de celulares estarem em constante procura e contato com pontos de acesso próximos. O histórico de redes conectadas pode ajudar a comprometer a privacidade do usuário.

• Dê sempre preferência para softwares livre e/ou de código aberto, pois, como seus códigos podem ser auditados por qualquer um que tenha o conhecimento técnico, no longo prazo, ocultar backdoors e outras práticas questionáveis se tornam muito difíceis. Ainda, vulnerabilidades podem ser mais facilmente detectadas. No modelo de código fechado, deve-se confiar completamente na palavra do desenvolvedor, e vulnerabilidades apenas são descobertas pela comunidade quando exploradas.

• A partir desse nível, não é recomendada a utilização de sistemas operacionais Windows e MacOS, por serem softwares proprietários de código fechado e não apresentarem bom histórico de respeito à privacidade do usuário. Mesmo que melhorias possam ser feitas, não se deve confiar nesses sistemas caso as demandas forem mais exigentes.

• Recomenda-se o uso de sistemas operacionais Linux, como o PopOS, Mint e PureOs. O Ubuntu, mesmo sendo superior ao Windows, é inferior quando se trata de privacidade aos anteriormente citados, portanto, não será aqui recomendado.

• Ataques que ligam a câmera do computador, sem que haja nenhuma indicação visual, podem ser facilmente mitigados com algo que as tampe, como um acessório especialmente para esse propósito, ou mesmo uma simples fita isolante. É recomendado também tampar a câmera frontal dos celulares, apenas destampando quando precisar usá-las.

• Caso não queira utilizar uma VPN, ao menos altere o seu provedor de DNS para uma alternativa mais privada, como o serviço da Quad9. Tente sempre escolher serviços de DNS presentes no Brasil, pois uma conexão com IP e DNS em países diferentes pode chamar atenção.

• Evite carregar seus dispositivos em locais desconhecidos ou públicos. Falsas estações de recarga infectam e roubam dados dos dispositivos enquanto carregam. Opções mais seguras são a utilização de power banks e/ou conectores que impeçam a transmissão de dados, mas liberem o fluxo de energia, como os fabricados pela PortaPow.

• Por padrão, as conversas no Telegram não são criptografadas de ponta a ponta. Para habilitar essa opção, deve-se entrar no contato que se deseja inciar um novo chat criptografado. Clique na parte superior, na foto ou nome/número do contato e clique nos três pontos no canto superior direito. Por fim, clique na opção “Iniciar Chat Secreto”.

• Como todas as imagens publicamente acessíveis na internet são escaneadas por inteligência artificial, limite o envio e compartilhamento de fotos, principalmente de rosto.

• A utilização de SSDs dificulta a certeza de remoção permanente de dados presentes no armazenamento. Com HDDs, esse problema é mais facilmente resolvido. Para os HDDs, pode-se utilizar o BleachBit (o software utilizado pela equipe de Hillary Clinton para apagar os e-mails comprometedores do escândalo de 2016). Para isso, nos três riscos horizontais, nas preferências, habilite a opção de sobrescrever para impedir a recuperação de dados. Os SSDs devem dispor da opção de TRIM. Em todos os casos, reinstalar o sistema operacional com criptografia total do armazenamento pode mitigar o problema da incerteza. Uma distribuição Linux com opção de criptografia já no processo de instalação é o PopOS.

• O software VeraCrypt é utilizado para criar cofres criptográficos. Com ele, pode-se criptografar partições ou dispositivos por completo. Recomenda-se que todos os dispositivos de transporte e backups, como pendrives, cartões de memória e HDDs externos sejam criptografados. No computador, também é possível criar cofres virtuais criptografados dentro de arquivos específicos.

• A compartimentalização e o aprofundamento em camadas devem ser utilizados extensivamente nesse e no próximo nível. Logo, por exemplo, para contas de e-mail, recomenda-se que o usuário tenha uma conta exclusiva para cada tarefa, como compras digitais, assuntos de trabalho/educação, ativismo digital, etc.

• O uso de pseudônimos é recomendado, uma nova conta devendo ser criada para cada um. Os navegadores também devem ser compartimentalizados, bem como os tipos de conexão (IP residencial, VPN, Tor, etc.). Novas identidades não precisam ter o mesmo gênero ou outras características que apontem para você. Não quebre as divisões entre os diferentes perfis. Destruir é muito mais fácil que construir, uma identidade cuidadosamente construída podendo ser comprometida rapidamente, caso as barreiras não sejam sempre respeitadas.

• Um excelente serviço para a criação de contas de e-mail para a compartimentalização é o SimpleLogin, recentemente adquirido pelo time da Proton. Com ele, é possível criar endereços de e-mail ligados a uma caixa de entrada escolhida pelo usuário. Para não revelar o verdadeiro e-mail do usuário, novos endereços são criados; todas as mensagens enviadas para eles serão encaminhadas para a caixa de entrada do e-mail escolhido, agindo como um proxy. As respostas também seguem a mesma lógica. Assim, os serviços são incapazes de acessar o endereço verdadeiro.

• Não coloque o Tor browser em tela cheia, pois, como a proteção do anonimato passa pela homogeneidade de todos os usuários, essa ação o tornará menos anônimo.

• Não conecte dispositivos de origem duvidosa, como pendrives desconhecidas encontradas por você.

• Evite nomear seu computador com seu nome verdadeiro, pois essa informação é compartilhada com os outros dispositivos na rede, também podendo ser transmitida pela internet, como metadado presente nos e-mails enviados.

• No recebimento de pacotes pelo correio, rasgue a etiqueta com as suas informações antes de jogar a caixa fora. Para documentos confidenciais, rasgue e distribua em diferentes latas de lixo. Queimá-los também é uma opção.

• Nas configurações de notificação, limite as que são exibidas na tela de bloqueio, pois, mesmo com o celular bloqueado, informações podem vazar pelas notificações exibidas.

• Lembre-se que, mais do que cada um em isolado, o par representa a verdadeira ameaça. Identidade sem informação não tem importância. Informação sem identidade se torna inútil.

Apêndice A (alternativas recomendadas)

- Adobe Reader →Calibre, Okular
- Adobe Photoshop → GIMP, Inkscape
- CCleaner →BleachBit
- Gmail, Outlook → Disroot, Mailfence, ProtonMail, Tutanota
- Google, Bing → Brave Search, DuckDuckGo, LibreX, MetaGer, SearchX, Startpage
- Google Chrome, Edge → Brave Browser (modificado), Firefox (modificado), LibreWolf, Tor Browser
- Google Docs → CryptPad
- Google Drive, Photos, OneDrive → Cryptee, Ente, Filen, Internxt, Sync, Nextcloud, pCloud, Proton Drive
- Google Maps → Open Street Map
- Google Meet, Skype, Slack → Element, Jami, Jitsi Meet, Wire, Zulip
- Google Tradutor → DeepL
- LastPass, Dashlane → KeePassXC
- Microsoft Office → LibreOffice, OnlyOffice
- Virus Total → Jotti
- Youtube → Odysee, Rumble
- Whatsapp → Telegram, Session, Signal, Status

FRONT-ENDS

- Google Tradutor → Lingva
- Medium → Scribe
- Reddit → Libreddit
- TikTok → ProxiTok
- Twitter → Nitter
- Youtube → FreeTube, Invidious

VPNs → IVPN, Mullvad e ProtonVPN (NUNCA, JAMAIS, utilize a Hola VPN).

Outros softwares/serviços recomendados

- 7zip
- Clementine
- Detwinner
- Dangerzone
- ExifCleaner
- Fluent Reader
- FreeCAD
- Joplin
- Notes-UP
- NoScript
- OpenSnitch
- Simple Login
- Standard Notes
- Shotcut
- uBlock Origin
- VeraCrypt

Android

- Aegis
- Aurora Store
- Bromite
- Cryptocam
- DroidFS
- F-droid
- InviZible Pro
- NetGuard
- NewPipe
- Open Camera
- Pdf Viewer Plus
- Photok
- RethinkDNS
- Safe Notes
- Simlar
- Simple Mobile Tools
- Yet Another Call Blocker

Apêndice B (modificação do arquivo de hosts)

Modificações no arquivo de hosts mitigam conexões não apenas em um navegador, mas no sistema como um todo. Alguns sites podem não funcionar como o esperado. No Linux, procure pelo arquivo de hosts utilizado pelo sistema. Na pasta “etc”, com permissão de administrador, adicione ao seu arquivo hosts:

- 0.0.0.0 ads.facebook.com
- 0.0.0.0 ads.google.com
- 0.0.0.0 ads.linkedin.com
- 0.0.0.0 ads.pubmatic.com
- 0.0.0.0 ads.rubiconproject.com
- 0.0.0.0 adservice.google.com
- 0.0.0.0 advertising-api-eu.amazon.com
- 0.0.0.0 advertising.twitter.com
- 0.0.0.0 advice-ads.s3.amazonaws.com
- 0.0.0.0 analytics.facebook.com
- 0.0.0.0 analytics.tiktok.com
- 0.0.0.0 analytics.twitter.com
- 0.0.0.0 analyticsengine.s3.amazonaws.com
- 0.0.0.0 assets-tracking.crazyegg.com
- 0.0.0.0 assets.adobedtm.com
- 0.0.0.0 assets.anytrack.io
- 0.0.0.0 assets.revcontent.com
- 0.0.0.0 c.amazon-adsystem.com
- 0.0.0.0 capture.trackjs.com
- 0.0.0.0 cdn.brandmetrics.com
- 0.0.0.0 cdn.cookielaw.org
- 0.0.0.0 cdn.onesignal.com
- 0.0.0.0 cdn.quantummetric.com
- 0.0.0.0 cdn.revcontent.com
- 0.0.0.0 cdn.taboola.com
- 0.0.0.0 click.google-analytics.com
- 0.0.0.0 connect.facebook.net
- 0.0.0.0 doubleclick.net
- 0.0.0.0 google-analytics.com
- 0.0.0.0 googleads.g.doubleclick.net
- 0.0.0.0 googleadservices.com

- 0.0.0.0 graph.facebook.com
- 0.0.0.0 hotjar-analytics.com
- 0.0.0.0 js-agent.newrelic.com
- 0.0.0.0 js.adsrvr.org
- 0.0.0.0 js.hs-analytics.net
- 0.0.0.0 js.hs-scripts.com
- 0.0.0.0 js.hsadspixel.net
- 0.0.0.0 js.juicyads.com
- 0.0.0.0 js.matheranalytics.com
- 0.0.0.0 mc.yandex.ru
- 0.0.0.0 pagead2.googlesyndication.com
- 0.0.0.0 pagestates-tracking.crazyegg.com
- 0.0.0.0 partner.googleadservices.com
- 0.0.0.0 px.ads.linkedin.com
- 0.0.0.0 px.moatads.com
- 0.0.0.0 pixel-apac.rubiconproject.com
- 0.0.0.0 pixel-eu.rubiconproject.com
- 0.0.0.0 pixel-geo.prfct.co
- 0.0.0.0 pixel-sync.sitescout.com
- 0.0.0.0 pixel-us-east.rubiconproject.com
- 0.0.0.0 pixel-us-west.rubiconproject.com
- 0.0.0.0 pixel.advertising.com
- 0.0.0.0 pixel.facebook.com
- 0.0.0.0 pixel.quantserve.com
- 0.0.0.0 pixel.rubiconproject.com
- 0.0.0.0 pixel.snapsmedia.io
- 0.0.0.0 pixel.tapad.com
- 0.0.0.0 pixel.wp.com
- 0.0.0.0 pubads.g.doubleclick.net
- 0.0.0.0 s.amazon-adsystem.com
- 0.0.0.0 securepubads.g.doubleclick.net

- 0.0.0.0 ssl.google-analytics.com
- 0.0.0.0 static.doubleclick.net
- 0.0.0.0 static.hotjar.com
- 0.0.0.0 stats.g.doubleclick.net
- 0.0.0.0 survey.g.doubleclick.net
- 0.0.0.0 track.adform.net
- 0.0.0.0 track.customer.io
- 0.0.0.0 track.dictionary.com
- 0.0.0.0 track.hubspot.com
- 0.0.0.0 tracker.bt.uol.com.br
- 0.0.0.0 tracker.metricool.com
- 0.0.0.0 tracking-api.hotmart.com
- 0.0.0.0 tracking-api.passeidireto.com
- 0.0.0.0 tracking.bloomberg.com
- 0.0.0.0 tracking.crazyegg.com
- 0.0.0.0 tracking.epicgames.com
- 0.0.0.0 usage.trackjs.com
- 0.0.0.0 whos.amung.us
- 0.0.0.0 widgets.outbrain.com
- 0.0.0.0 www.google-analytics.com
- 0.0.0.0 www.googleads.g.doubleclick.net
- 0.0.0.0 www.googleadservices.com
- 0.0.0.0 www.googleoptimize.com
- 0.0.0.0 www.googletagmanager.com
- 0.0.0.0 www.googletagservices.com
- 0.0.0.0 z-na.amazon-adsystem.com

Caso algum serviço por você utilizado apresente problemas, basta remover a linha referente à conexão bloqueada.

Apêndice C (hardening de sistemas Linux)

Como sempre, modifique o seu sistema por sua conta e risco.

Procure pelo firewall presente no sistema. Caso ele estiver desabilitado habilite-o. Caso utilize o ufw (Uncomplicated Firewall), deixe o “incoming” como “Deny” e “Outgoig” como “Allow”. Nas regras, você poderá adicionar aquelas que lhe serão benéficas, como rejeitar conexões SSDP, por exemplo.

Caso você não precise utilizar serviços, como o avahi-daemon e o cups-browsed, para se conectar à impressoras em sua rede, por exemplo, deixe-os desligados. Para impedir conexões realizadas pelo avahi-daemon, entre, com permissão de administrador em: etc → avahi → avahi-daemon.conf.

- Altere:
  - use-ipv4=yes → no
  - use-ipv6=yes → no
- No terminal:
  - sudo service avahi-daemon restart
- Você poderá reverter essas mudanças caso precise futuramente.
- Pode-se utilizar um firewall adicional, como o OpenSnitch, para bloquear conexões de certos aplicativos ou apenas analisar as conexões sendo realizadas.
- Ao instalar Flatpaks, utilize o FlatSeal para avaliar as permissões que eles possuem.
- Atualize seus softwares. Uma forma recomendada é utilizar o Synaptic Package Manager.
- Ao utilizar uma VPN, certifique-se de que não há vazamento de DNS. Testes desse tipo podem ser feitos pelos sites:
  - https://www.dnsleaktest.com/
  - https://ipleak.net/
  - https://browserleaks.com/ip
- Verifique as configurações de sua conexão e altere o DNS caso for preciso.
- No terminal, digite:
  - sudo apt install apparmor-profiles apparmor-utils
  - sudo aa-enforce /etc/apparmor.d/*
- Para verificar, digite:
  - sudo aa-status
- Instale o chkrootkit:
  - sudo apt install chkrootkit
- Para verificar, digite:
  - sudo chkrootkit
- Instale o rkhunter:
  - sudo apt install rkhunter
- Para verificar, digite:
  - sudo rkhunter --check --enable rootkits --skip-keypress
- Instale o clamav:
  - sudo apt install clamav

- Para verificar, digite:
  - sudo find / -name “*.*” -mtime -7 -type f -print0 | sudo xargs -0 clamscan --detect-pua=yes –log=/var/log/clamscan.log
- O parâmetro “-7” indica, em dias, o período decorrido da modificação do conteúdo do arquivo. Pode ser substituído por “ctime”, que é parecido com “mtime”, também sendo alterado quando se altera o anterior, além de quando são alteradas as permissões, nome ou localização do arquivo. O parâmetro “*.*” deve ser substituído pelo nome ou extensão do arquivo. Por exemplo, caso eu queira verificar todos os arquivos .pdf modificados nos últimos 5 dias, o comando deve ser alterado para:
  - sudo find / -name “*.pdf” -ctime -5 -type f -print0 | sudo xargs -0 clamscan --detect-pua=yes –log=/var/log/clamscan.log
- Outras opções podem ser encontradas em:
  - clamscan --help
- Para desativar o IPv6, além de alterar as configurações da sua conexão atual, adicione, ao final do arquivo “etc/sysctl.conf”, as seguintes linhas:
  - net.ipv6.conf.all.disable_ipv6 = 1
  - net.ipv6.conf.default.disable_ipv6 = 1
  - net.ipv6.conf.lo.disable_ipv6 = 1
- Pode ser editado com VIM:
  - vim /etc/sysctl.conf
- Para alterar o endereço MAC, instale o MacChanger pelo comando:
  - sudo apt install macchanger
- Para alterar o endereço MAC, escolha uma interface. Você pode utilizar o comando “ifconfig” no terminal. Após escolher a interface, digite:
  - sudo macchanger -r interface
- Verifique a modificação do MAC executando novamente o “ifconfig”. Faça isso antes de se conectar à rede.

Apêndice D (hardening do Firefox)

Clicando nos três riscos no canto superior direito, entre nas configurações. Em privacidade em segurança, mude o modo de proteção para estrito. Desabilite armazenamento de senhas e preenchimento automático. Nunca lembrar histórico. Desabilite a coleta de dados. Habilite o modo HTTPS em todas as janelas. Desabilite a Proteção contra conteúdo enganoso e softwares perigosos, pois o Firefox realiza comunicações constantes com os servidores da Google para poder utilizar esse serviço. Em busca, altere o buscador padrão para o DuckDuckGo.

As modificações a partir daqui efetuadas poderão quebrar alguns sites. Na barra de

endereços, digite about:config e aceite o risco. Altere os seguintes parâmetros:

- beacon.enabled = false
- browser.cache.disk_cache_ssl = false
- browser.cache.offline.enable = false
- browser.link.open_newwindow.restriction = 0
- browser.newtabpage.activity-stream.feeds.telemetry = false
- browser.ping-centre.telemetry = false
- browser.safebrowsing.blockedURIs.enabled = false
- browser.safebrowsing.downloads.remote.enabled = false
- browser.send_pings = false
- browser.send_pings.max_per_link = 0
- browser.sessionstore.resume_from_crash = false
- browser.zoom.siteSpecific = false
- device.sensors.enabled = false
- dom.battery.enabled = false
- dom.caches.enabled = false
- dom.disable_window_move_resize = true
- dom.event.clipboardevents.enabled= false
- dom.push.connection.enabled = false
- dom.push.enabled = false
- dom.storage.enabled = false
- full-screen-api.enabled = false
- geo.enabled = false
- layout.css.visited_links_enabled = false
- media.navigator.enabled = false
- media.peerconnection.enabled = false
- media.peerconnection.turn.disable = true
- media.peerconnection.use_document_iceservers = false
- media.peerconnection.video.enabled = false
- media.video_stats.enabled = false
- media.webspeech.synth.enabled = false
- pdfjs.enableScripting = false

- privacy.firstparty.isolate = true
- privacy.resistFingerprinting = true
- security.ssl.enable_false_start = false
- toolkit.telemetry.unified = false
- toolkit.telemetry.server = vazio
- webgl.disabled = true

Para o LibreWolf:

- browser.cache.disk_cache_ssl = false
- browser.cache.memory.enable = false
- browser.cache.offline.enable = false
- browser.send_pings.max_per_link = 0
- browser.sessionstore.resume_from_crash = false
- browser.zoom.siteSpecific = false
- device.sensors.enabled = false
- dom.battery.enabled = false
- dom.caches.enabled = false
- dom.event.clipboardevents.enabled = false
- dom.push.connection.enabled = false
- dom.push.enabled = false
- dom.storage.enabled = false
- full-screen-api.enabled = false
- geo.enabled = false
- layout.css.visited_links_enabled = false
- media.navigator.enabled = false
- media.peerconnection.enabled = false
- media.peerconnection.turn.disable = true
- media.peerconnection.use_document_iceservers = false
- media.peerconnection.video.enabled = false
- media.video_stats.enabled = false
- security.ssl.enable_false_start = false

Apêndice E (limpeza com ADB)

Primeiramente, obtenha status de desenvolvedor. O processo é ligeiramente diferente para cada modelo de celular, mas, geralmente, deve-se clicar repetidas vezes em algo como a versão do dispositivo, nas informações do sobre o telefone. Uma vez obtidas as opções de desenvolvedor, habilite a depuração por USB. Permita e aceite.

Será utilizado o software ADB para a remoção de aplicativos nativos, os bloatwares que vêm junto com o seu aparelho. Aqueles aplicativos que você não usa, mas não consegue desinstalar. Um aviso, apenas desinstale aplicativos que não geram problemas, como os não necessários para o funcionamento do aparelho. Pode ser necessário pesquisar sobre o seu aparelho em específico. Caso acabe desinstalando um aplicativo importante por engano, poderá haver a necessidade de formatar o dispositivo. Me pergunte como eu sei.

A descrição a seguir trata do uso do ADB nas distribuições Linux baseadas em Debian.

- Com os passos anteriores executados, conecte o celular ao computador. Abra o terminal de sua distribuição e digite os seguintes comandos:
  - sudo apt install adb
  - adb devices
  - adb shell
- Aceite os pedidos que aparecerem no dispositivo. Para desinstalar os aplicativos desejados, utilize o seguinte comando:
  - pm uninstall --user 0 com.nomedopacote
  - caso queira manter os arquivos de usuário, adicione -k após o “pm uninstall” (pm uninstall -k)
- ou:
  - pm disable-user com.nomedopacote
- para desabilitar os aplicativos escolhidos.

Nos dois casos, altere a parte final do comando para o pacote de sua escolha. O nome do pacote não é o mesmo do aplicativo. Paradescobrir o nome do pacote, abra “configurações” => “apps” => “gereciar apps” => selecione o aplicativo => clique no “i” no canto superior direito. O nome que você deverá inserir no comando está em “nome do APK”.

Contanto que não desinstale aplicativos importantes para o sistema, ou alguns sabidamente problemáticos (procure nos fóruns relativos ao seu dispostivo), não haverá grandes problemas. Em todo o caso, é recomendado realizar backup prévio. A

escolha pelos aplicativos que desejar desinstalar é subjetiva. No caso da Xiaomi, recomendo desinstalar, principalmente, o “com.miui.analytics” e o “com.miui.msa.global”, basicamente, spywares integrados ao sistema.

Quando terminar, para sair, digite “exit”.

Terminada essa etapa, instale a loja de aplicativos F-droid. Você poderá instalar pelo site do projeto, efetuando o download do APK. Alguns aplicativos desinstalados por você nas etapas anteriores não necessitam de substitutos, contudo, você poderá substituir aplicativos úteis por alternativas presentes no F-droid, como a câmera e o navegador.

Com eles, você poderá controlar quais aplicativos terão acesso à internet, o que reduz, por si só, substancialmente a quantidade de informações enviadas por seu dispositivo a servidores remotos espalhados pelo mundo. Como ainda estamos na ROM proprietária do fabricante, essa etapa se torna ainda mais importante. Nem todos os aplicativos que gostaríamos de desinstalar são realmente possíveis sem quebrar o sistema.

O InviZible Pro é o mais recomendado dos três, por ser multifuncional. Com ele, é possível bloquear seletivamente a conexão de aplicativos à internet (por meio do firewall interno), seletivamente rotear a conexão de aplicativos pela rede Tor, bem como seletivamente bloquear o acesso a sites e domínios, já que possibilita a edição e importação de arquivos de host.

Tecnologia